STUDENT COMPUTER AND INTERNET USE RULES

These rules accompany Board policy IJNDB (Student Computer and Internet Use). Each student is responsible for his/her actions and activities involving school unit computers, networks and Internet services, and for his/her computer files, passwords and accounts. These rules provide general guidance concerning the use of the school unit's computers and examples of prohibited uses. The rules do not attempt to describe every possible prohibited activity by students. Students, parents and school staff who have questions about whether a particular activity is prohibited are encouraged to contact a building administrator or the Technology Manager.

A. Consequences for Violation of Computer Use Policy and Rules

Student use of the school unit computers, networks and Internet services is a privilege, not a right. Compliance with the school unit's policies and rules concerning computer use is mandatory. Students who violate these policies and rules may have their computer privileges limited, suspended or revoked. Such violations may also result in disciplinary action, referral to law enforcement and/or legal action.

The building principal shall have the final authority to decide whether a student's privileges will be limited, suspended or revoked based upon the circumstances of the particular case, the student's prior disciplinary record and any other pertinent factors.

B. Acceptable Use

The school unit's computers, networks and Internet services are provided for educational purposes and research consistent with the school unit's educational mission, curriculum and instructional goals.

All Board policies, school rules and expectations concerning student conduct and communications apply when students are using computers.

Students are also expected to comply with all specific instructions from teachers and other school staff or volunteers when using the school unit's computers.

C. Prohibited Uses

Examples of unacceptable uses of school unit computers that are expressly prohibited include, but are not limited to, the following:

1. **Accessing or Communicating Inappropriate Materials** - Accessing, submitting, posting, publishing, forwarding, downloading, scanning or displaying defamatory, abusive, obscene,

STUDENT COMPUTER AND INTERNET USE RULES

vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing and/or illegal materials or messages.

2. **Illegal Activities -** Using the school unit's computers, networks and Internet services for any illegal activity or in violation of any Board policy or school rules. The school unit assumes no responsibility for illegal activities of students while using school computers.

3. **Violating Copyrights** – Copying, downloading or sharing any type of copyrighted materials (including music or films) without the owner's permission (see Board policy/procedure EGAD – Copyright Compliance). The school unit assumes no responsibility for copyright violations by students.

4. **Copying Software** - Copying or downloading software without the express authorization of the Technology Manager. Unauthorized copying of software is illegal and may subject the copier to substantial civil and criminal penalties. The school unit assumes no responsibility for illegal software copying by students.

5. **Plagiarism** - Representing as one's own work any materials obtained on the Internet (such as term papers, articles, music, etc). When Internet sources are used in student work, the author, publisher and web site must be identified.

6. **Non-School-Related Uses** - Using the school unit's computers, networks and Internet services for non-school-related purposes such as private financial gain; commercial, advertising or solicitation purposes; or any other personal use not connected with the educational program or assignments.

7. **Misuse of Passwords/Unauthorized Access** - Sharing passwords, using other users' passwords, and accessing or using other users' accounts; or attempting to circumvent network or computer security systems.

8. **Malicious Use/Vandalism** - Any malicious use, disruption or harm to the school unit's computers, networks and Internet services, including but not limited to hacking activities and creation/uploading of computer viruses.

9. **Avoiding School Filters** – Attempting to or using any software, utilties, or other means to access Internet sites or content blocked by the school filters.

10. **Unauthorized Access to Blogs/Chat Rooms** – Accessing blogs, social networking sites, etc to which student access is prohibited. Such sites may only be used under the direction of a supervising teacher.

STUDENT COMPUTER AND INTERNET USE RULES

D. No Expectation of Privacy

Mt. Blue R.S.D.'s computers remain under the control, custody and supervision of the school unit at all times. Students have no expectation of privacy in their use of school computers, including e-mail, stored files and Internet access logs.

E. Compensation for Losses, Costs and/or Damages

The student and his/her parents are responsible for compensating the school unit for any losses, costs or damages incurred by the school unit for violations of Board policies and school rules while the student is using school unit computers, including the cost of investigating such violations. The school unit assumes no responsibility for any unauthorized charges or costs incurred by a student while using school unit computers, including but not limited to credit card charges, long distance telephone charges, equipment and line costs, or for any illegal use of its computers, such as copyright violations.

F. Student Security

A student is not allowed to reveal his/her full name, address, telephone number, social security number or other personal information on the Internet without prior permission from a teacher. Students should never agree to meet people they have contacted through the Internet without parental permission. Students should inform their teacher if they access information or messages that are dangerous, inappropriate or make them uncomfortable in any way.

G. System Security

The security of the school unit's computers, networks and Internet services is a high priority. Any student who identifies a security problem must notify his/her teacher immediately. The student shall not demonstrate the problem to others or access unauthorized material. Any user who attempts to breach system security, causes a breach of system security or fails to report a system security problem shall be subject to disciplinary and/or legal action in addition to having his/her computer privileges limited, suspended or revoked.

H. Additional Rules for Laptops Issued to Students

1. Laptops are loaned to students as an educational tool and are only authorized for use in completing school assignments.
2. Before a laptop is issued to a student, the student and his/her parent must sign the school's acknowledgment form.

STUDENT COMPUTER AND INTERNET USE RULES

3. Students and their families are responsible for the proper care of laptops at all times, whether on or off school property, including costs associated with repairing or replacing the laptop. **Mt. Blue R.S.D. offers a protection plan for parents to cover replacement costs and/or repair costs for accidental damages not covered by the laptop warranty. Parents should be aware that they are responsible for any costs associated with loss, theft, or damage to a laptop issued to their child.**

4. If a laptop is lost or stolen, this must be reported to the building administrator immediately. If a laptop is stolen, a report should be made to the local police and Technology Manager immediately.

5. The Board's policy and rules concerning computer and Internet use apply to use of laptops at any time or place, on or off school property. Students are responsible for obeying any additional rules concerning care of laptops issued by school staff.

6. Violation of policies or rules governing the use of computers, or any careless use of a laptop may result in a student's laptop being confiscated and/or a student only being allowed to use the laptop under the direct supervision of school staff. The student will also be subject to disciplinary action for any violations of Board policies or school rules.

7. Parents are responsible for supervising their child's use of the laptop and Internet access when in use at home.

8. The laptop may only be used by the student to whom it is assigned and family members to the extent permitted by the MLTI program. Any family member using the laptop must abide by all school board policies and school rules.

9. Laptops must be returned in acceptable working order at the end of the school year or whenever requested by school staff.

I. Use of Privately-Owned Computers by Students

1. A student who wishes to use a privately-owned computer in school must make a request in writing to the Technology Director and building principal. The request must be signed by both the student and a parent or guardian. There must be an educational basis for any request.

2. The Technology Director will determine whether the student's privately-owned computer meets the school unit's network requirements.

3. Requests may be denied if it is determined that there is not a suitable educational basis for the request and/or if the demands on the schools unit's network or staff would make it unreasonable.

STUDENT COMPUTER AND INTERNET USE RULES

4. The student is responsible for proper care of his/her privately-owned computer, including any costs of repair, replacement, or any modifications needed to use the computer at school.

5. The school unit is not responsible for damage, loss, or theft of any privately-owned computer.

6. Students are required to comply with all Board policies, administrative procedures and school rules while using privately-owned computers at school.

7. Students have no expectation of privacy in their use of a privately-owned computer while at school. The school unit reserves the right to search a student's privately-owned computer is there is a reasonable suspicion that the student has violated Board policies, administrative procedures, or school rules, or engaged in other misconduct while using the computer.

8. Violation of Board policies, administrative procedures or school rules involving a student's privately-owned computer may result in the revocation of the privilege of using the computer at school and/or disciplinary action.

9. The school unit may confiscate any privately-owned computer used by a student in school without authorization as required by these rules. The contents of the computer may be searched in accordance with applicable laws and policies.

Cross Reference: IJNDB – Student Computer and Internet Use
Adopted: June 13, 2000
Reviewed: March 26, 2002
Revised: February 28, 2006
Revised: October 27,2009
Revised: April 6, 2010

STUDENT COMPUTER AND INTERNET USE RULES